Math 3032 Lecture 3 (Jan 19, 2021)

theojf@dal.ca

Reminder: HW 1 due Thursday (end of day). Single page PDF submit via email.

Office hours same as last week: Thu 1-3. This might change.

Each of you should introduce yourself to me sometime this week. Either show up at office hours or email me to find a time.

Today: more on homomorphisms + units + zero divisors.

<u>Defn</u>: Let R and S be rings. A <u>ring homomorphism</u> from R to S is a function $f: R \to S$ s.t. $\forall r_1, r_2 \in R$,

$$f(r_1 + r_2) = f(r_1) + f(r_2) \quad \text{and} \quad f(r_1 \cdot r_2) = f(r_1) \cdot f(r_2)$$

operations in R operations in S

<u>N.B:</u> $\Rightarrow f(0) = 0$.
$f(-r) = -f(r)$

Sometimes rings are assumed to be unital. A <u>unital homomorphism</u> is one which moreover satisfies $f(1) = 1$.

unit in R unit in S.

"mathematicians' non". ← not necessarily.

<u>Vocab</u>: A <u>category</u> is a collection of mathematical objects and the maps between them.

E.g. {gps}, {nonunital rings}, {unital rings}.

Lemma: Suppose a homomorphism $f: R \to S$ is bijective, i.e. $\forall s \in S$, $\exists$ unique $r \in R$ s.t. $f(r) = s$.

Then f is invertible: there is a homomorphism $f^{-1}: S \to R$ s.t. $f \circ f^{-1} = id_S$, $f^{-1} \circ f = id_R$.

In other words, f is an isomorphism.

Pf: Because f is bijective, there is a unique function f^{-1} which might work. Namely, $f^{-1}(s) :=$ the unique r s.t. $f(r) = s$.

The only question is: is f^{-1} a homomorphism?

E.g. $f^{-1}(s_1 \cdot s_2) \stackrel{?}{=} f^{-1}(s_1) \cdot f^{-1}(s_2)$

$$\Longleftrightarrow s_1 \cdot s_2 = f(f^{-1}(s_1 \cdot s_2)) \stackrel{?}{=} f(f^{-1}(s_1) \cdot f^{-1}(s_2)) = f(f^{-1}(s_1)) \cdot f(f^{-1}(s_2))$$

$\underset{\shortparallel}{s_1} \cdot s_2 .\checkmark$

Ring homomorphisms with domain $\mathbb{Z}$.

A group homomorphism $f:(\mathbb{Z},+)\to(S,+)$ is uniquely determined by $f(1)\in S$, $f(1) = a$. "$(\mathbb{Z},+)$ is the free gp on one generator".

$n>0$

$$n = \underbrace{1+1+\dots+1}_{n} \longmapsto \underbrace{a+a+\dots+a}_{n}.$$

$1^2=1$. If f is to be a ring hom, $f(1)^2 = f(1^2) = f(1)$, so $a^2 = a$.

"a is idempotent"

$$\{\text{Ring homs } f:\mathbb{Z}\to S\} \hookrightarrow \{\text{idempotents in } S\}$$

$$\cap \qquad\qquad\qquad\qquad \cap$$

$$\{\text{gp homs } \mathbb{Z}\to S\} \xrightarrow{\sim} S$$

$$f \longmapsto f(1)$$

In fact, this is a bijection.

Claim: If $a \in S$ is idempotent, then the gp homomorphism

$$f: \mathbb{Z} \to S$$
$$1 \mapsto a$$
$$n \mapsto \underbrace{a + \dots + a}_{n}$$

is a ring homomorphism.

Cor: If S is unital, then there is a unique unital homomorphism $\mathbb{Z} \to S$. $\hom_{\text{un ring}}(\mathbb{Z}, S) = \{*\}$.

"$\mathbb{Z}$ is <u>initial</u> in {unital rings}"

Pf: $f(m \cdot n) \overset{?}{=} f(m) \cdot f(n)$.

Case I: $m, n > 0$.

$$\underbrace{a + a + \dots + a}_{m \cdot n} \overset{?}{=} \overbrace{\underbrace{(a + \dots + a)}_{m}}^{m \cdot a} \underbrace{(a + \dots + a)}_{n} = \underbrace{a^2 + a^2 + \dots + a^2}_{m \cdot n} \checkmark.$$

Case II: $m > 0$, $n < 0$. Then $f(m \cdot n) = f(-m \cdot |n|)$

$$= -f(m \cdot |n|) \overset{I}{=} -f(m) \cdot f(|n|) = f(m) \cdot f(-|n|).$$

$\mathbb{Z}_n$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}/(n)$

Ring homomorphisms with domain $\mathbb{Z}/n$.

Gp homomorphisms $f: (\mathbb{Z}/n, +) \to (S, +)$ are determined by $f(1)$. But not every choice works. $f(1)$ must have order dividing n.

Punchline: $\mathrm{Hom}_{\text{rings}}(\mathbb{Z}/n, S) \overset{\sim}{\longleftrightarrow}$ idempotents in S of additive order dividing n.

$$\mathrm{Hom}_{\text{rings}}(\mathbb{Z}/n, S) = \{\text{ring homs } \mathbb{Z}/n \to S\}$$

$$\mathrm{Hom}_{\substack{\text{unital}\\ \text{rings}}}(\mathbb{Z}/n, S) = \begin{cases} \emptyset & \text{if } n\cdot 1 \neq 0 \\ \boxed{\text{one element} \quad \text{if } n\cdot 1 = 0.} \end{cases}$$

S has characteristic n.

"$\mathbb{Z}/n$ is initial in $\{$unital rings of char. $n\}$."

"CRT" **Chinese Remainder Thm:** Suppose m and n are relatively prime. There is a (unique) ring isomorphism

$$\mathbb{Z}/(mn) \cong \mathbb{Z}/m \times \mathbb{Z}/n.$$

E.g. $\mathbb{Z}/18 \cong \mathbb{Z}/9 \times \mathbb{Z}/2$.

Pf: It suffices to give a bijective homomorphism

$$\mathbb{Z}/mn \longrightarrow (\mathbb{Z}/m \times \mathbb{Z}/n) = \{(p,q) \text{ where } p \in \mathbb{Z}/m,\ q \in \mathbb{Z}/n\}$$

Such a homorphism exists and unique iff $mn(1,1) = 0$ in RHS.

$$mn(1,1) = (mn, mn) \overset{?}{=} 0$$

$mn \overset{?}{\equiv} 0 \pmod m$ ✓.

$mn \overset{?}{\equiv} 0 \pmod n$ ✓.

Last thing to check is that this map is a bijection.

You already did that in 3031.

(uses that you can solve $pm + qn = 1$)

More on zero divisors.

Recall that $a \in R$ is a (left) zero divisor if $\exists\, b \neq 0$ s.t. $ab = 0$. (ba?)

E.g.: 0 is a zero divisor. Non e.g.: units are never zero div.

In a unital ring "the unit" is the mult. id. $1 \in R$. the units are the $r \in R$ s.t. $\exists\, r^{-1}$ w/ $rr^{-1} = r^{-1}r = 1$. $R^\times$.

Lemma: Iff a is not a (left) zero divisor, then you can cancel (left) multiplication by a. I.e. $ab = ac \Rightarrow b = c$.

Pf: Suppose a not a zero div. and $ab = ac$.

Then $\underset{\overset{\parallel}{a(b-c)}}{ab - ac} = 0$. So $b - c = 0$.

Converse: If a is a zero div, choose b as and $ab = 0$. $\not\Rightarrow b = 0$.

In particular, having no zero divisors in R

$\Rightarrow$ nonzero mult is cancelative in R.

Theorem: Suppose R is a <u>finite</u> unital ring. Then every element of R is either $\underbrace{\text{a unit}}_{\text{invertible.}}$ or a zero divisor.

N.B: Not generally true for infinite rings.

Pf: Consider the set $\left\{ \begin{array}{l} \text{elements of } R \\ \text{which are not zero divisors} \end{array} \right\} =: G \supseteq R^{\times}$

$R \supseteq G$, $\quad R^{\times} = \{\text{invertibles}\}$

Claim: G is a gp. under $\times$ in R.

- $1 \in G$
- closed? If $a, b \in G$, wts $ab \in G$.

  If it isn't, then $\exists\, c \neq 0$ s.t. $\underset{= a(bc)}{(ab)c} = 0 \underset{\substack{\text{because} \\ a \in G}}{\Rightarrow} bc = 0 \Rightarrow c = 0$

Pick $a \in G$, consider $a, a^2, a^3, \ldots \in G$. Since $|G| < \infty$, this sequence must repeat itself. (Pigeonhole)

$a, a^2, \ldots \in G$ must repeat. I.e. $\exists\ i<j$

s.t. $a^i 1 = a^i = a^j = a^i \cdot a^{j-i}$ in R.

But $a^i \in G$, so a is cancellative. So $1 = a^{j-i}$

So $a^{j-i-1} \in G$ is an inverse to a. $\square$

(Compare: A closed subset of a finite gp is a subgp).

"FLT"

<u>Corollary</u> <u>[Fermat's little theorem]:</u> Let p a prime.

Then $a^{p-1} \equiv 1 \mod p$ $\forall \underset{\mathbb{Z}}{\overset{\uparrow}{a}} \notin p\mathbb{Z}$, and $a^p \equiv a$ $\forall a \in \mathbb{Z}$

<u>Pf:</u> This is a statement in $\mathbb{Z}/p$. (Namely that "$a^{p-1} = 1$ in $\mathbb{Z}/p$.")

$(\mathbb{Z}/p)^\times = \underset{\text{divisors}}{\text{non-zero}} = \mathbb{Z}/p \setminus \{0\}$. order $p-1$.

This is a gp under mult.

For any finite gp G, $g^{|G|} = 1$ $\forall g \in G$.

Defn: Euler's totient function, aka Euler's φ-function

is $\varphi(n) = |(\mathbb{Z}/n)^\times|$ = number of $k < n$ $\underbrace{\text{(co)prime}}_{\text{rel. prime.}}$ to n.

<u>Generalization of FLT</u>: If $\underbrace{\overset{\gcd(a,n)}{(a,n)} \equiv 1}_{\Updownarrow\ [a] \in (\mathbb{Z}/n)^\times.}$, then $a^{\varphi(n)} \equiv 1 \ (n)$.

By the way, what is the function φ?

- $\varphi(p) = p-1$ if p is prime.
- $\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$.
- $\varphi(mn) = \varphi(m)\varphi(n)$ if $(m,n) = 1$. $\Leftarrow$ CRT.